UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/456,794	12/08/1999	JAY C. CHEN	34581/CAG/C718	6924

7590 09/29/2003

McDermott Will & Emery
Attn: Craig A. Gelfound
2049 Century Park East
34th FL
Los Angeles, CA 90067-3208

EXAMINER
MEISLAHN, DOUGLAS J

ART UNIT	PAPER NUMBER
2132	12

DATE MAILED: 09/29/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/456,794	CHEN, JAY C.	
	Examiner	Art Unit	
	Douglas J. Meislahn	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 July 2003* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *81-116* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *81-116* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 December 1999* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 03 July 2003 that cancelled claims 54-80 and amended claims 81, 84, 89, 96, 98, 99, 102, 103, 109, and 113.

Response to Arguments

2. Applicant's arguments with respect to claims 81-116 have been considered but are moot in view of the new ground(s) of rejection. Applicant's main argument is that the cited prior art does not show one of the entities in the transaction uniquely generating the session key. The Woo-Lam protocol does indeed show one of the parties to the transaction receiving the session key from a third party. However, there is no explicit teaching of why external generation of the session key is beneficial to the system.

Drawings

3. The drawings are objected to because elements 1-10 in figure 2 and 50 and 1180 in figure 12 are not labeled. Correction is required. Numbers do not count as labels.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 54, 55, 81 rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboorg et al. (6240091) in view of Schneier.

In lines 51-67 of column 7, Ginzboorg et al. present a smart card that includes, among other pieces of data, the public key of a second party. As evidenced by the abstract and billing system (BS) in figure 3a, Ginzboorg et al. complete a transaction. They do not teach the specific steps of the claims. In describing the Woo-Lam protocol described on page 64, Schneier shows, in step 3, Alice initiating communications with Bob by encrypting a message (Bob's name and a random challenge) with Bob's public key and sending it to him. He then encrypts Trent's signature, which contains K, with Alice's public key, thereby formatting a key exchange response message, and sends it to her. Alice uses the session key to encrypt Bob's challenge (sent with Trent's signature), and the transaction is completed. Schneier's method provides authentication and a symmetric key. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the teachings of Schneier in Ginzboorg et al.'s system so as to both authenticate parties and in order to provide the parties with a symmetric key.

The Woo-Lam protocol does not task Bob with uniquely generating the session key. In a basic encrypted key exchange protocol where the session key is to be exchanged, described on page 518, step 2, Bob uniquely generates the session key. While not discusses in this session, the benefits of Bob himself generating the session key include minimizing the number of times that the session key is transmitted. Although encrypted, transmitting the session key from Trent to Bob in the Woo-Lam

protocol presents a small vulnerability, that being interception and successful illicit decryption of the key. A second vulnerability is that Trent is not actually trustworthy and will maliciously use the session key against Bob and Alice. The benefit of using Trent to generate the session key lies largely in Trent theoretically being trusted as competent in producing session keys. Some cryptanalytic attacks make use of pockets of determinism in key generation. These risks are known to people of ordinary skill in the art. So, the decision to generate the session key internally or externally should be based on the parties' assessment of the trade-off between the risks. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for Bob to internally generate the session key instead of using a session key received from Trent. By internally making the key, Bob would protect the key from interception and cracking and a dishonest Trent.

6. Claims 56-74 and 82-102 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboorg et al. in view of Schneier as applied to claims 54, 55, and 81 above, and further in view of Walker et al. (6263438).

Ginzboorg et al. and Schneier teach a smart card that contains a second entity's public key. The smart card and second entity authenticate themselves to one another and agree on a symmetric key. There is no teaching of sending the smart card's public key to the second entity. In lines 38-52 of column 6, Walker et al. teach including digital certificates (which include encrypted forms of an originator's public key) with messages to provide greater assurance. Therefore it would have been obvious to a person of

ordinary skill in the art at the time the invention was made to send a certificate with Alice's first message, as taught by Walker et al., to provide greater assurance.

As this applies to the claims, 56 is clearly rendered obvious. Step 5 in the Woo-Lam protocol involves the second entity providing a challenge, meeting addition limitations of claim 57. Schneier teaches signing messages on pages 576 and 577. Ginzboorg et al. also teach signatures in, for example, their abstract. This renders obvious signing all messages sent from one entity to another. 58 is obvious because of this teaching and the additional payment steps shown by Ginzboorg et al.

Ginzboorg et al., Schneier, and Walker et al. do not mention using the symmetric key to protect information, such as account information, a transaction amount, and sensitive transaction data. Official notice is taken that it is old and well known for a purchaser to encrypt data, including account information, a transaction amount, and sensitive transaction data, with a symmetric key in an electronic transaction in order to prevent that data from being used illicitly. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt transaction data sent between the two entities in order to protect data. Data that need not be protected should not be, thereby reducing cryptographic operations and meeting the limitations of claims 60 and 62.

Ginzboorg et al., Schneier, and Walker et al. has not mandated that the entities include transaction identifiers with their transaction correspondences. Official notice is taken that it is old and well known to include transaction identifiers assigned by one entity with their transaction correspondences, which helps catalog and identify

messages. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include transaction identifiers with their transaction correspondences in order to track messages.

7. Claims 75-80 and 103-116 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboorg et al., Schneier, and Walker et al. as applied to claim 54 above, and further in view of Thompson et al.

Ginzboorg et al., Schneier, and Walker et al. teach a method for exchanging keys. They do not show the group method of key request. Thompson et al show a method by which changes to a document are recorded. This method entails signing all changes. For the purposes of this discussion, we will assume that Thompson et al.'s original bill corresponds to applicant's key exchange request. As can be seen in figure 5, the original bill has been signed by the originator and then modified and signed by a second entity, whereby the original bill remains perceptible. The benefit of this is that it allows parties to know exactly what different entities added, as taught in lines 29 and 30 of column 5. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include signatures and recognizable updates as taught by Thompson et al. in Schneier's key exchange requests, thereby piggybacking requests and reducing the total number of transmissions of data.

Different session keys would be the most obvious, as the requesting entities have made no indication of wanting to communicate with each other. However, a scenario where two requesting entities desired the same key so that they could communicate securely is also obvious.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100